How do you configure a Virtual Local Area Network (VLAN) in PCS 7?

SIMATIC PCS 7 V9.0 / SCALANCE XC-200

https://support.industry.siemens.com/cs/ww/en/view/66807297

Siemens Industry Online Support

This entry originates from Siemens Industry Online Support. The conditions of use specified there apply (www.siemens.com/nutzungsbedingungen).

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. The customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity. Siemens' products and solutions undergo continuous development. Siemens recommends that you keep yourself regularly informed about product updates.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. Implemented products from other manufacturers are also to be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats. More information about this is available under http://www.siemens.com/industrialsecurity.

Contents

1 Using VLANs in PCS 7

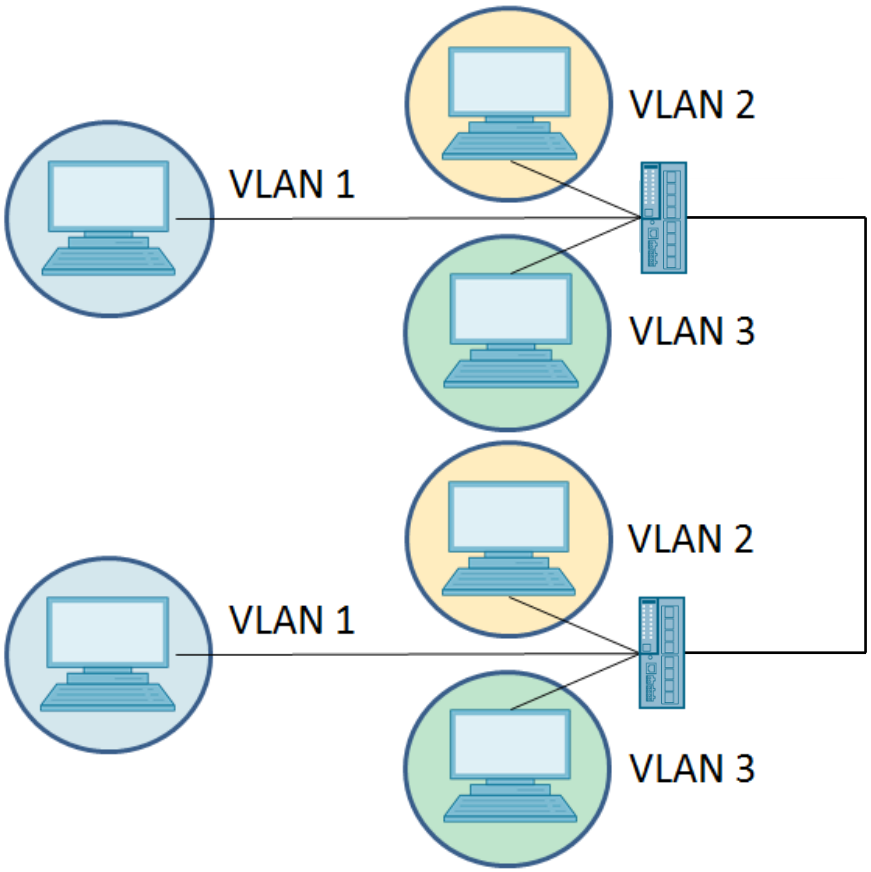
In the following we give you an overview of the use and structure of VLAN technology in the PCS 7 environment. In addition we describe how to configure the VLANs taking the example of a SCALANCE XC-200 switch.
Configuration instructions taking the example of a SCALANCE X-300 switch are available at the following link:
https://support.industry.siemens.com/cs/ww/en/view/66807297

Note There are restrictions on the use of VLANs in PCS 7.
The use of a redundancy connection via VLAN is not recommended for the sake of availability among other things. This might lead to unexpected or undesirable plant behavior.

What is a VLAN?

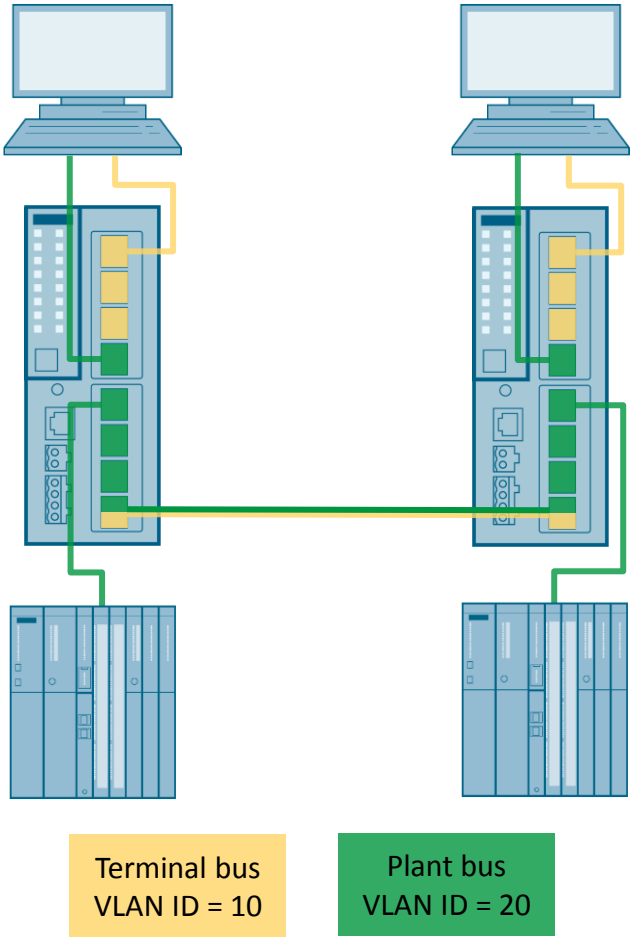
A Virtual Local Area Network (VLAN) is a logical subnetwork. This subnetwork can be assigned to a switch or be an entire physical network.

Figure 1-1



The subnetwork can extend beyond one or more switches. VLANs segment physical networks into logical subnetworks. Here, VLAN-compatible switches split up the frames (data packages) between the separate VLANs. The frames are not forwarded to another VLAN even though the subnetworks might be connected to common switches.

Figure 1-2



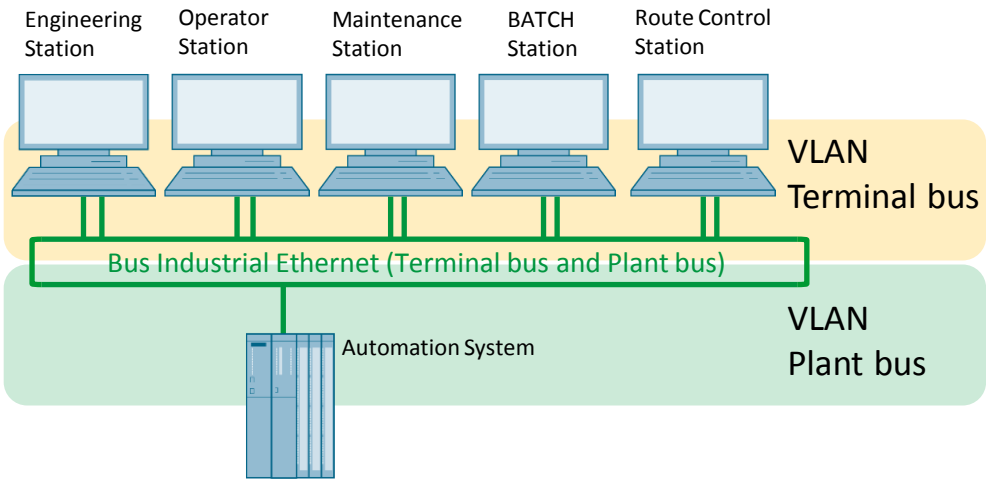
More information about VLANs is available in the following application example:
"Segmenting a Network Using VLANs"
https://support.industry.siemens.com/cs/ww/en/view/109749844

When do you use VLANs in PCS 7?

The use of VLANs in the PCS 7 environment is limited to the applications below.

- **Combined plant and terminal bus**
  This architecture consists of just one physical Ethernet network that is used for both the plant bus and the terminal bus. VLAN separates these two network levels on a logical level. By using a common medium, the networks might influence one another. The separation of communication networks recommended for PCS 7 is achieved on a logical level.
- **VMware ESXi server in virtual infrastructures**
  In virtual infrastructures various PC stations (OS clients, for example) are virtualized together on one server. This means that not all the PC stations have to be physically present.

Figure 1-3



Further information about the requirements for a combined plant and terminal bus are available in the following FAQ response:
"What are the requirements for operating PCS 7 via common plant and terminal buses?"
https://support.industry.siemens.com/cs/ww/en/view/43273606

Which devices are needed for using VLANs?

VLAN-compatible switches are needed for using VLANs in the PCS 7 environment. The following switches from the Siemens product portfolio support port-based VLANs with tagged frames:

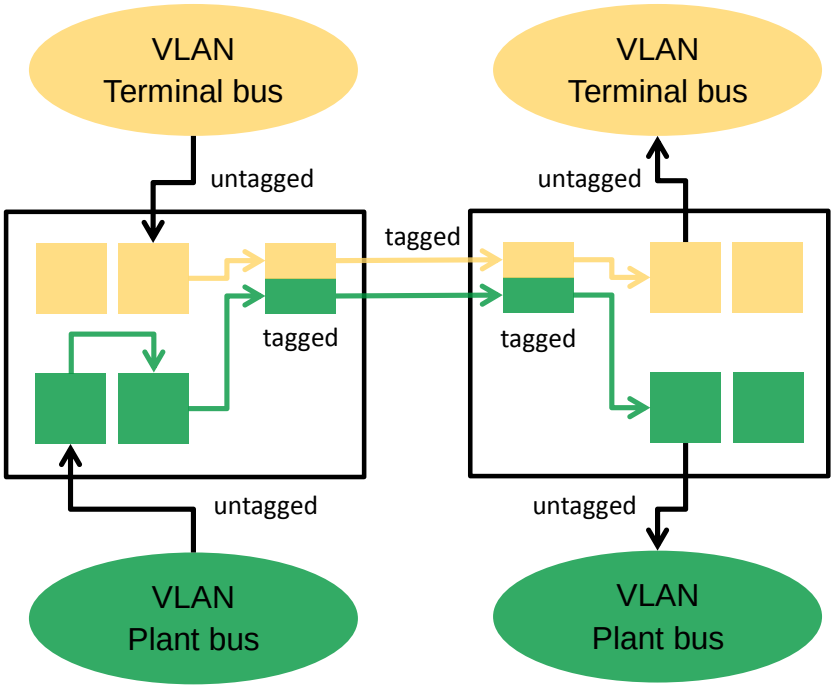
- SCALANCE XC-200
- SCALANCE XP-200
- SCALANCE XF-204-2BA
- SCALANCE X-300
- SCALANCE X-400
- SCALANCE X-500

When you configure the switch you define which VLAN is assigned to which port of the switch and therefore also the nodes connected to it. The port-specific VLAN tags serve as identification.

- A VLAN tag is added to a message (Ingress) when received on the switch from a terminal node.
- A VLAN tag is removed from a message (Egress) when sent from the switch to a terminal node.

In the case of communication between two switches (Trunk) the VLAN tags are not removed when leaving the switch. When received, the VLAN tags are retained in the partner switch which ensures that the VLANs remain separated.

Tagged messages are always used within the switch.



Further information is available in the application example:
"Segmenting a Network Using VLANs"
https://support.industry.siemens.com/cs/ww/en/view/109749844

2 VLAN Configuration for Use in PCS 7

The following configuration instructions describe how to create two static VLANs for a terminal bus and a plant bus.

Before configuring the VLANs, you should make sure that the criteria for creating at least two or more VLANs are met.

Proceed as follows for the planning:

1. Define the criteria for creating at least two or more VLANs and any VLAN priorities.
2. Assign the nodes to the separate VLANs.
3. Create a configuration list.
4. Define to which device and at which port there is a connection.

We show the example of configuring the VLANs on a SCALANCE XC208 switch, according to Table 2-1.
Port P0.8 is planned as trunk or connection to another switch via which the VLANs extend themselves.

Table 2-1 VLAN configuration

Port	VLAN ID	Use
P0.1	10	Terminal bus
P0.2	10	Terminal bus
P0.3	10	Terminal bus
P0.4	20	Plant bus
P0.5	20	Plant bus
P0.6	20	Plant bus
P0.7	20	Plant bus
P0.8	Trunk	Connection to another switch

The following essential steps must be made for configuring the VLANs in the switch:

1. Configuration of the VLAN mode.
2. Definition of the VLANs.
3. Definition of how the messages are to be processed at the input and output sides of the port (ingress and egress filters).

Note Refer to the following manual for more configuration parameters: "SIMATIC NET: Industrial Ethernet Switches SCALANCE XB-200/XC-200/ XF 200BA/XP-200/XR-300WG Web Based Management"
https://support.industry.siemens.com/cs/ww/en/view/109757421

Note This document describes the VLAN configuration taking the example of a SCALANCE XC-200 switch. Configuration instructions taking the example of a SCALANCE X-300 switch are available at the following link:
https://support.industry.siemens.com/cs/ww/en/view/66807297

2.1 Ring Redundancy

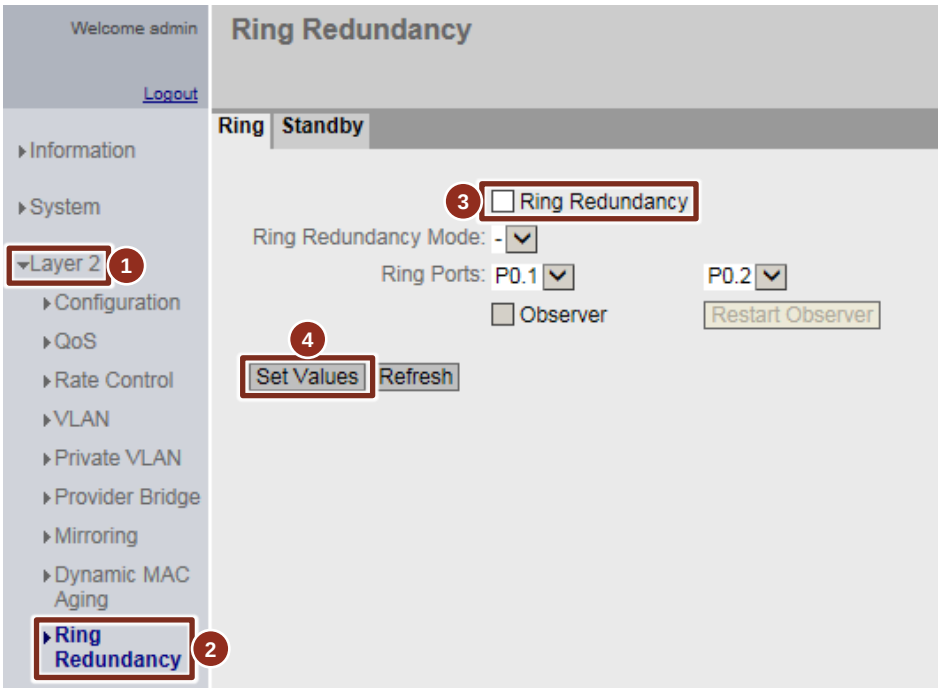
In the standard configuration (factory settings) of a SCALANCE XC-200 switch the ring redundancy is enabled and set to "Automatic Redundancy Detection" for ports P0.1 and P0.2.

In the following, the ring redundancy is disabled, because ports P0.1 and P0.2 are to be configured later for the VLAN terminal bus (VLAN ID 10).

If, as an alternative, you wish to create a ring of switches, you configure the corresponding ring redundancy and then both ring ports as trunks (see section 2.7).

Procedure

1. Connect your PC with the switch.
   In the following, access is via Port 1, because during the configuration temporary settings for this port are made, sections 2.5 and 2.7.
2. Call the Web Based Management in your browser using the IP address of the switch.
3. Log on as Administrator.
4. Navigate to the menu "Layer 2 > Ring Redundancy" (1), (2).
5. Disable the "Ring Redundancy" option (3).
6. Confirm the settings with the "Set Values" button (4).



Result

The ring redundancy is disabled.

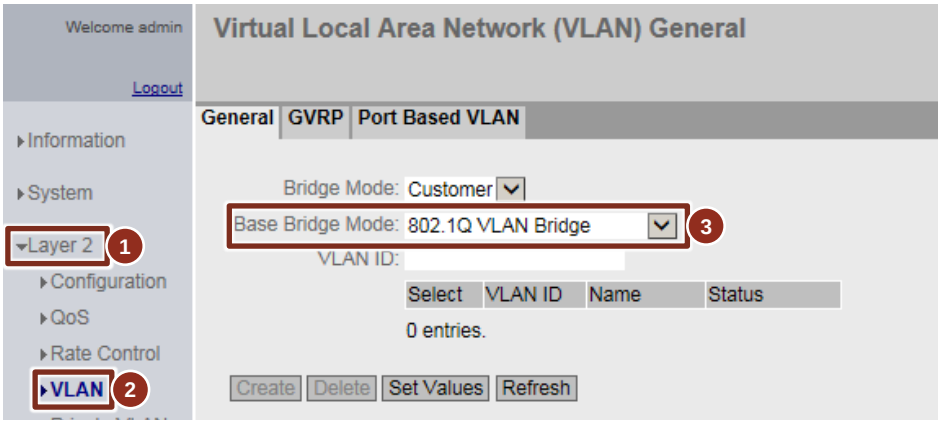
2.2 Configuration of the VLAN Mode

The requirement for configuration of the port-based VLANs is that the Base Bridge Mode is set as "802.1Q VLAN Bridge". This mode is also known as "VLAN-aware", which means that VLAN information is taken into account in the switch. With this setting VLANs and use of the ports can be defined.

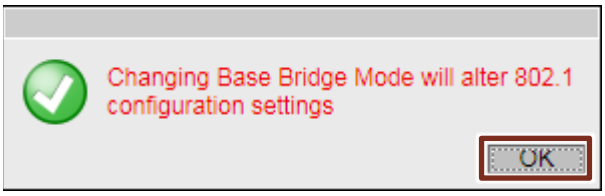
In the other Base Bridge Mode "802.1D Transparent Bridge", also known as "VLAN-unaware", VLAN tags are not changed, but are forwarded transparently.

Configuration of the Base Bridge Mode "802.1Q VLAN Bridge"

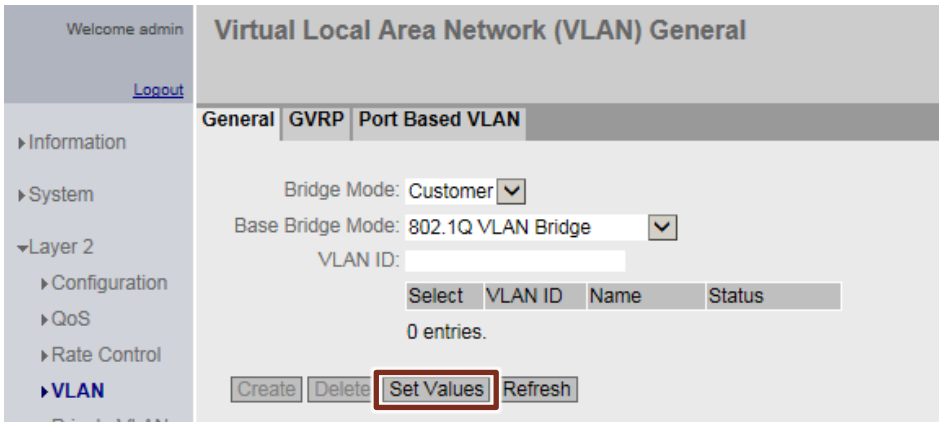
1. Navigate to the menu "Layer 2 > VLAN" (1), (2).
2. Select the "General" tab and in the Base Bridge Mode drop-down list box you select "802.1Q VLAN Bridge" (3).



3. A message is displayed indicating that changing the mode will alter the 802.1 settings. Confirm the message with "OK".



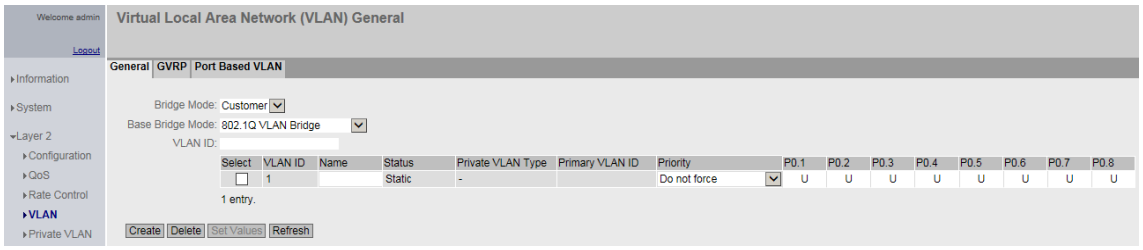
4. Confirm the settings with the "Set Values" button (4).



Result

The VLAN mode is set to "802.1Q VLAN Bridge". The Management VLAN (VLAN ID 1) has been created and is displayed in the list. The VLAN ID 1 is set with the option "U" (untagged) by default for all ports. This means that all the ports on the device send messages by default without VLAN tag. These can be also be received by nodes that do not support VLAN.

Figure 2-1



Note

The VLAN with VLAN ID 1 is available by default and is used as the Management VLAN. An IP interface is always configured for this VLAN, via which the Web Based Management among other things can be accessed. In order to access the switch via another VLAN you have to create another IP interface, see section 2.4.

The Management VLAN has another special feature in the configuration of the ring redundancy. Ring ports have to be assigned to the Management-VLAN (VLAN ID 1), but they can also forward messages for other VLANs.

2.3 Definition of the VLANs

After configuring the VLAN mode you can define other VLANs.

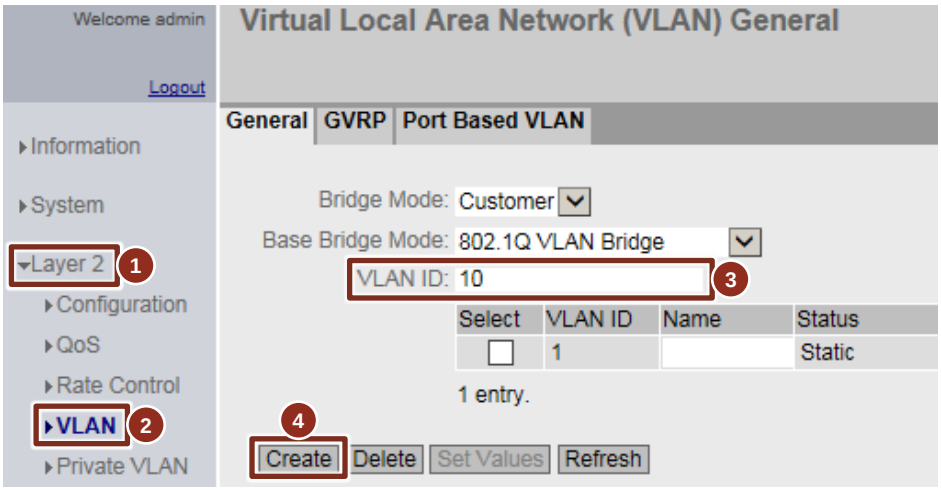
Partitioning into the following VLANs is planned for the separation of plant bus and terminal bus:

- Terminal bus: VLAN ID 10
- Plant bus: VLAN ID 20

The VLAN IDs 10 and 20 have been selected as examples. Generally, you can use any VLAN ID in the range of 2 to 4094. In the following we describe how to proceed to create VLANs.

Procedure

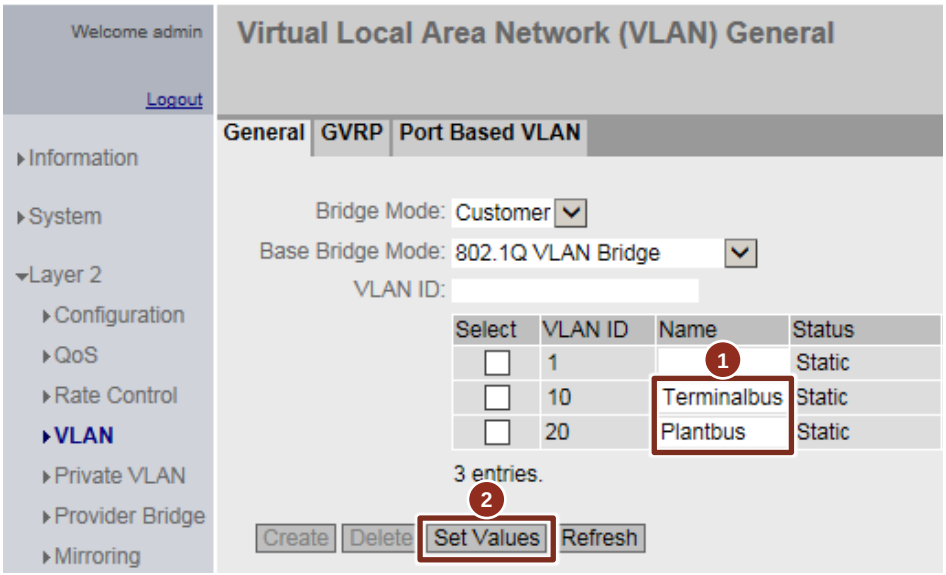
1. Navigate to the menu "Layer 2 > VLAN" (1), (2).
2. Enter a VLAN ID for the VLAN to be created, for example "10" (3).
3. Click the "Create" button (4) to create the VLAN for the terminal bus.



4. Repeat steps 1 to 3 to create another VLAN, this time for the plant bus.

5. You also have the option to enter names for the VLANs (1):
   - VLAN ID 10: "Terminal bus"
   - VLAN ID 20: "Plant bus"

   Confirm the name changes with the "Set Values" button (2).



Note If necessary, you can assign a priority of between 0 and 7 (highest) to the VLAN. With the setting "Do not force" the priority of the messages remains unchanged.

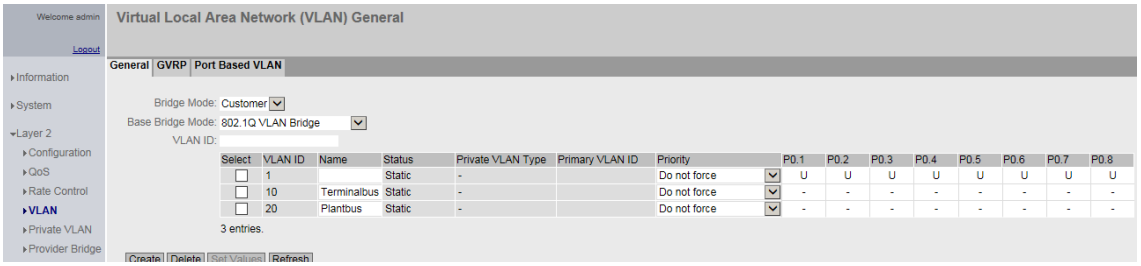
Result

The following VLANs are created:

- VLAN ID 1: Management VLAN
- VLAN ID 10: Terminal bus
- VLAN ID 20: Plant bus

The option "-" is set by default at all the ports of the new VLANs. With this setting none of the messages of the VLANs are forwarded via these ports.

Figure 2-2



2.4 Configuration of the IP Interface

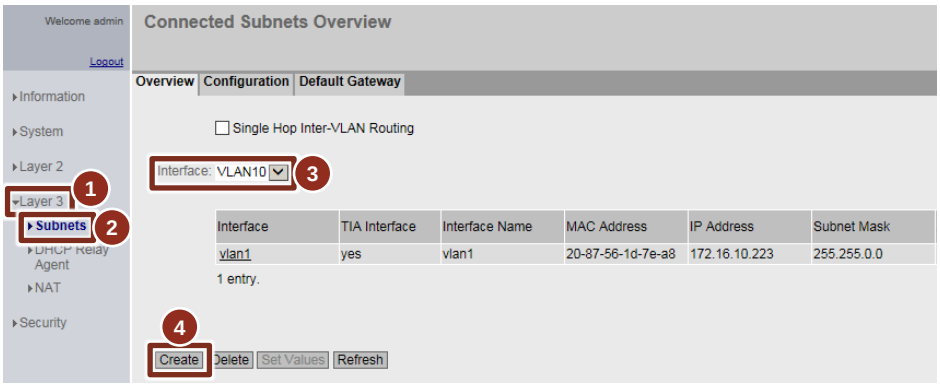
In the standard configuration of the switch it has only one IP interface that can be accessed in the "802.1Q VLAN Bridge" ("VLAN-aware") mode only via the Management VLAN (VLAN ID 1).

Since in the planned configuration of the switch, see Table 2-1, all the ports are specified for plant bus (VLAN ID 20) and terminal bus (VLAN ID 10), the switch could not be accessed for more configuration changes or diagnostics.

Therefore, in the following another IP interface is created for the terminal bus (VLAN ID 10). The Web Based Management can then be accessed via this IP interface and, among other things, inclusion in the Asset Management via SNMP is possible.

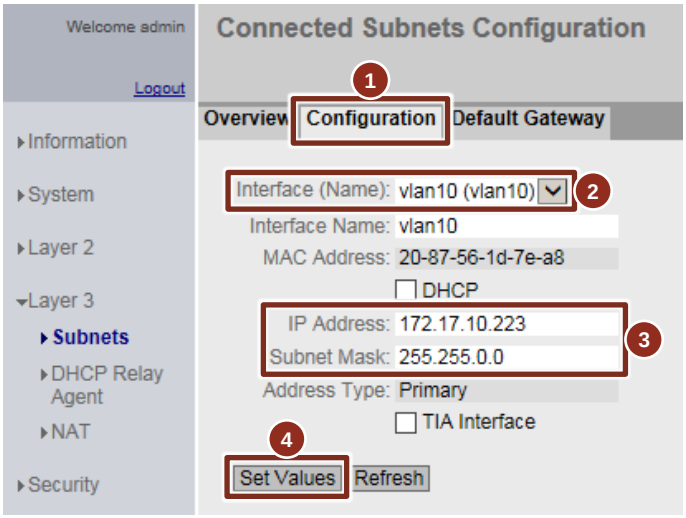
Procedure

1. Navigate to the menu "Layer 3 > Subnets" (1), (2).
2. From the "Interface" drop-down list box (3) you select the VLAN of the terminal bus (VLAN 10).
3. Click the "Create" button (4) to create the IP interface for the terminal bus.



4. Switch to the "Configuration" tab (1).
5. From the "Interface" drop-down list box (2) you select the VLAN of the terminal bus (VLAN 10).
6. In the fields "IP Address" and "Subnet Mask" (3) you enter the IP address and associated subnet mask via which the switch is to be accessible from the terminal bus VLAN.

7. Confirm the settings with the "Set Values" button (4).



Note The "TIA Interface" option enables or disables accessibility via the DCP protocol in the corresponding VLAN.

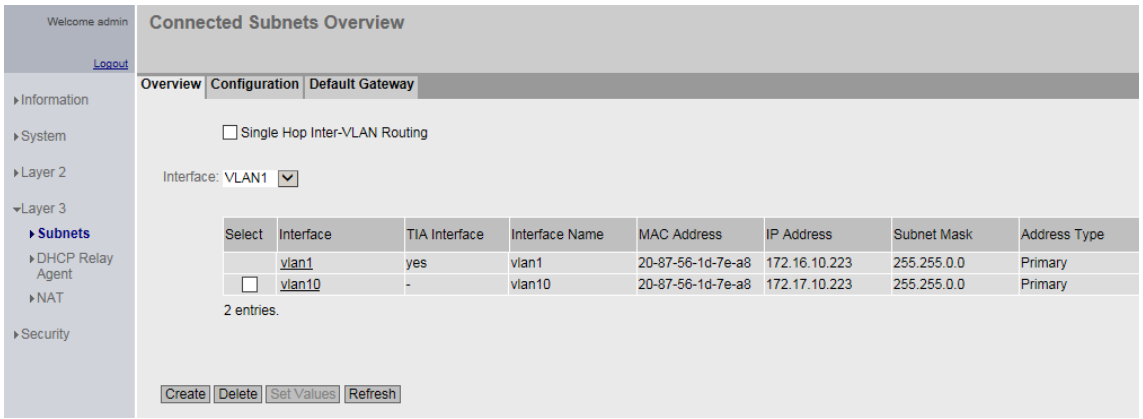
Result

There are two IP interfaces configured for the switch:

- Management VLAN (VLAN ID 1) 172.16.10.22 (255.255.0.0)
- Terminal bus VLAN (VLAN ID 10) 172.17.10.223 (255.255.0.0)

This means that the switch is now prepared to be also accessible from the terminal bus VLAN for configuration and diagnostics, via the WBM or SNMP, for example.

Figure 2-3



2.5 Egress Settings

In this step we define the utilization of the ports on the output (egress) side. This includes which VLAN messages may be forwarded via which ports and whether the VLAN tags are to be kept or removed.

Table 2-2 gives you an overview of the settings used for configuring the plant bus and terminal bus.

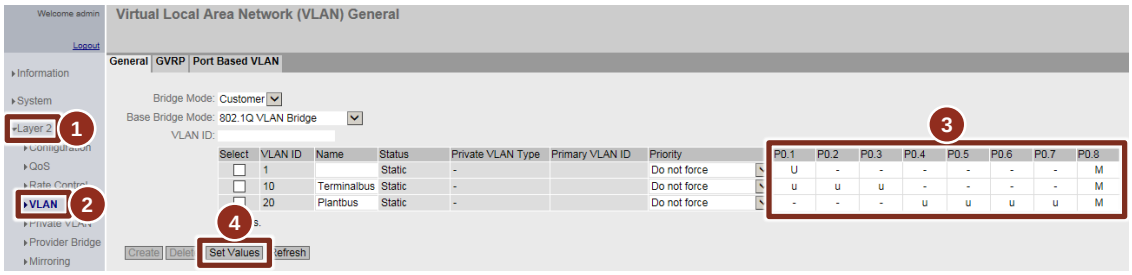
Table 2-2

Setting	Description
"-"	The port is not a member of the specified VLAN, which means that no messages of this VLAN are output at the port. In the case of a new definition all the ports are set with the ID "-".
M	The port is a member of the VLAN. Messages sent in this VLAN are forwarded with the corresponding VLAN tag.
U (uppercase letter)	The port is an untagged member of the VLAN, which means that the messages of this VLAN are sent after removal of the VLAN tag.
u (lowercase letter)	The port is an untagged member of the VLAN but the VLAN is not configured as Port VLAN (see section 2.6). The messages of this VLAN are sent after removal of the VLAN tag.

In the following the ports are configured as planned in Table 2-1.

Procedure

1. Navigate to the menu "Layer 2 > VLAN" (1), (2).
2. To configure a port, in the line of the VLAN to which the port is to be assigned you click the corresponding field.
   Select the required option from the drop-down list box (3).
   - **Ports with connections to terminal nodes: "U", "u" and "-"**
     Ports to which terminal nodes are connected (PCs, for example) are configured for a VLAN with "U" or "u". All other VLANs of the port are configured with "-".
     With this setting, at this port only the messages of the VLAN configured with "U" or "u" are forwarded. The VLAN tag is removed to ensure that all the devices can interpret the message.
   - **Ports with connections to other switches (trunks): "M"**
     Ports with connections to other switches (trunks) are configured with "M" for all VLANs. With this setting, at this port the messages of all VLANs that are configured are forwarded including the VLAN tag.
3. To ensure continuous accessibility of the WBM during configuration, the port via which you are connected with the switch has to be configured in addition as untagged member ("U") for VLAN 1 until the Ingress settings have been completed. We use port P0.1 in the following.
4. When you have configured all the ports, confirm the settings with the "Set Values" button (4).



Note

The lowercase "u" indicates that the Egress and Ingress settings are different on that port. In the Ingress setting a different VLAN ID is stored, with which the incoming messages are tagged. After the Ingress setting (see section 2.6) the setting changes to an uppercase "U".

Result

Port P0.1 is an untagged member of the Management VLAN (VLAN ID 1) and of the terminal bus (VLAN ID 10). This means that messages with VLAN ID 1 or 10 are forwarded via the port. Depending on the setting "U" or "u" (untagged) the VLAN tags of the outgoing messages are removed before being sent.
Ports P0.2 and P0.3 are untagged members of the terminal bus (VLAN ID 10). This means that only messages with VLAN ID 10 are forwarded via these ports. The VLAN tags are likewise removed before the messages are sent. In the same way the ports P0.4 to P0.7 are untagged members of the plant bus (VLAN ID 20).
Port P0.8 is configured for the connection to another switch, which means that it is a member in all VLANs and forwards outgoing messages with VLAN tag because of the setting "M".

Note If you configure VLANs in the switch, make sure that the port with which you are connected to the switch is also always assigned to a VLAN that has an IP interface. If you remove this port from the VLAN, the switch is no longer accessible. In this case you have to connect with another port that is assigned to a VLAN that has an IP interface.

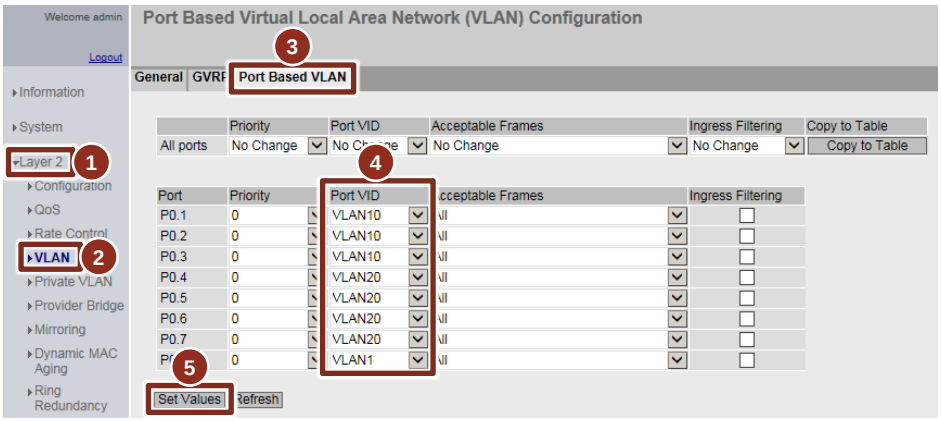
2.6 Ingress Settings

In this step we define the configuration of the ports on the input (ingress) side. This includes which VLAN ID and which priority are to be assigned to a message that arrives at this port and has no VLAN tag.

In the following the ports are configured as planned in Table 2-1.

Procedure

1. Navigate to the menu "Layer 2 > VLAN" (1), (2).
2. Switch to the "Port Based VLAN" tab (3).
3. To configure a port, in the line of the port to be configured you click in the corresponding field in the Port VID column. In the drop-down list box you see the standard VLAN and also all the VLANs that you have previously configured. Select the desired VLAN (4).
   - The ports assigned to the terminal bus have the Port VLAN ID of the terminal bus (VLAN10).
   - The ports assigned to the plant bus have the Port VLAN ID of the plant bus (VLAN20).
   - Ports for connections to other switches remain assigned to the Standard Management VLAN (VLAN1).
4. When you have configured all the ports, confirm the settings with the "Set Values" button (5).



Note The Ingress filter is disabled, which means that all the messages that already have a VLAN tag are forwarded unchanged via the port.

Result

The Port VLAN ID 10 is configured for ports P0.1 to P0.3. This means that incoming messages without VLAN tag receive a VLAN tag with VLAN ID 10. In the same way the ports P0.4 to P0.7 are configured for the plant bus (VLAN ID 20). Port P0.8 as connection to another switch continues to be assigned to the Management VLAN (VLAN ID 1).

Since the port P0.1 used for the configuration is assigned on the Ingress side to the Port VLAN ID 10, the IP interface of the Management VLAN (VLAN ID 1) used previously is no longer accessible via this port. The IP interface of the terminal bus (VLAN ID 10) created in section 2.4 is available for further access.

2.7 Complete the Configuration

After configuration of the Ingress settings, the IP interface of the Management VLAN (VLAN ID 1) used previously is no longer accessible via the port P0.1 (VLAN ID 10) used for the configuration. The IP interface of the terminal bus (VLAN ID 10) created in section 2.4 is available for further access. This is accessible via all the ports (P0.1 to P0.3) assigned to the terminal bus.

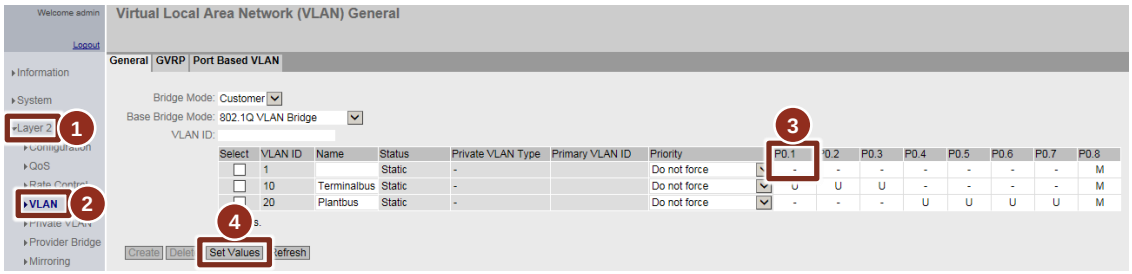
To complete the VLAN configuration, the temporary Egress setting for the port P0.1 used for the configuration as untagged member in VLAN 1 has to be removed.

Note

To access the IP interface of the terminal bus (VLAN ID 10) created in section 2.4 the configuration PC must have an IP address in the same IP address range as the interface.

Procedure

1. Connect your PC with a port of the switch that is assigned to the terminal bus VLAN.
2. With the IP address of the IP interface of the terminal bus (VLAN ID 10) created in section 2.4 you call the Web Based Management in your browser.
3. Log on as Administrator.
4. Navigate to the menu "Layer 2 > VLAN" (1), (2).
5. Remove the membership of the port used for the configuration in the Management VLAN (VLAN ID 1) by selecting "-" in the corresponding cell (3).
6. Confirm the settings with the "Set Values" button (4).



Result

The configuration of the VLANs for the terminal bus and plant bus is completed.

The networks are defined port for port and are separated logically. Direct communication between nodes of the plant bus and nodes of the terminal bus is not possible.